Exemplo de função. AS-FE-I-001-V10-PT

Sistemas de Controle Fail-safe

SIMATIC Safety Integrated

Parada de emergência com confirmação na categoria de segurança 4 conforme EN 954-1

safety INTEGRATED

SIEMENS

Nota prévia

Os exemplos de função relativos ao tema “Safety Integrated” são configurações de automação operacionais e testadas na base de produtos A & D standard para a execução fácil, rápida e econômica de exigências de automação na técnica de segurança. Cada um dos exemplos de função presentes representa a solução para uma exigência parcial freqüente de uma problemática típica apresentada pelo cliente dentro do setor da técnica de segurança.

Além da enumeração de todos os componentes necessários de software e hardware e da descrição da conexão destes, os exemplos de função contêm o código testado e comentado. Com isto, as funcionalidades aqui descritas podem ser reproduzidas num curto espaço de tempo, podendo assim ser utilizadas como base para ampliações individuais.

Nota importante

Os exemplos de função são facultativos e não pretendem ser completos quanto à configuração e ao equipamento bem como a todas as eventualidades. Os exemplos de função Safety não representam soluções específicas para os clientes, pretendendo apenas oferecer uma ajuda para a solução de exigências típicas. Você próprio é responsável pelo funcionamento adequado dos produtos descritos.

Estes exemplos de função Safety não dispensam da obrigação da utilização segura na aplicação, instalação, operação e manutenção. Através da utilização dos exemplos de função Safety você aceita a não responsabilidade da Siemens por danos eventuais para além do regulamento de responsabilidade acima descrito. Reservamo-nos o direito de efetuar alterações nestes exemplos de função Safety sem aviso prévio e a qualquer momento. Em caso de divergências entre as propostas nestes exemplos de função Safety e outras publicações da Siemens como p. ex. catálogos, tem prioridade o conteúdo da outra documentação.

Sumário

1 Garantia, responsabilidade e suporte

Não assumimos nenhuma garantia para as informações contidas neste documento.

A nossa responsabilidade, independentemente da causa jurídica, fica excluída no caso de danos causados através da utilização dos exemplos, avisos, programas, dados de projeção e de capacidade etc. descritos nestes exemplos de função Safety, a não ser que p. ex. conforme a Lei alemã sobre a responsabilidade civil do fornecedor pelo fato do produto (Produkthaftungsgesetz) a responsabilidade seja obrigatória em casos de intenção, de negligência grave, por causa de lesão à vida, ao corpo ou à saúde, por causa de uma aceitação de garantia para a qualidade de uma coisa, por causa de ocultação dolosa de um vício ou por causa da lesão de obrigações contratuais essenciais. A indenização devido à violação de obrigações contratuais essenciais limita-se porém ao dano típico contratual e previsível, a não ser que haja intenção ou negligência grave ou que a responsabilidade seja obrigatória por causa de lesão à vida, ao corpo ou à saúde. Não é relacionada a isto uma alteração do ônus da prova em seu detrimento.

Em caso de dúvidas relativas a este artigo, contate-nos através do seguinte endereço de e-mail :

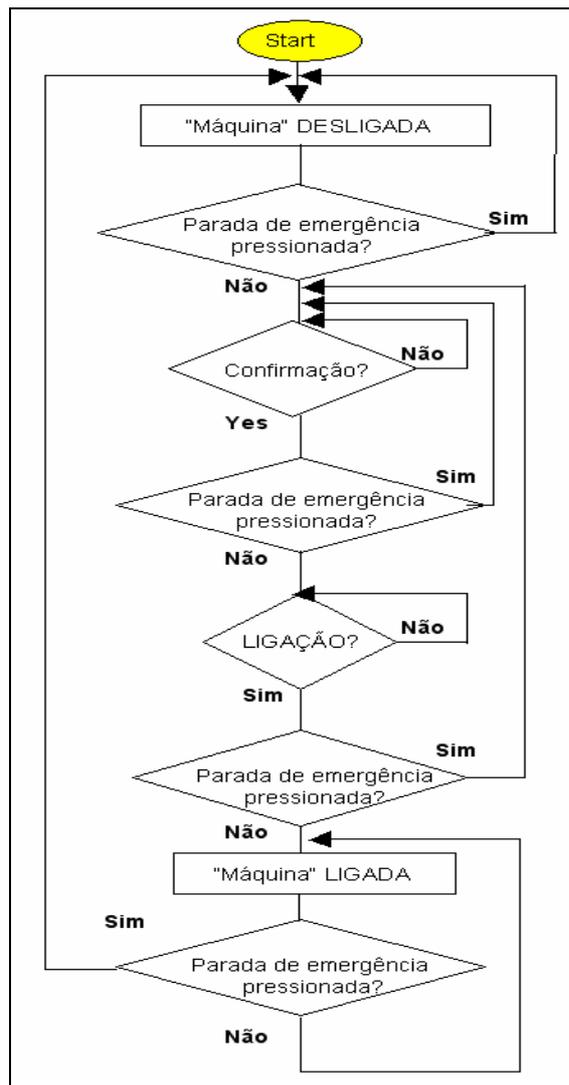
csweb@ad.siemens.de

2 Função de automação

2.1 Descrição da funcionalidade

Pessoas que se encontram (p. ex. na técnica de produção) próximas de máquinas, devem ser protegidas adequadamente por dispositivos técnicos. A parada de emergência representa uma medida de segurança suplementar para proteger pessoas e instalações de perigos. A parada de emergência deve ter prioridade em relação a todas as outras funcionalidades.

Dispositivos, aspectos funcionais e princípios de projeto relativos à parada de emergência encontram-se na norma **EN 418**; adicionalmente ainda tem de ser observada a norma **EN 60204-1** : **1997**.

No exemplo aqui apresentado uma chave de parada de emergência acionada desliga uma saída de um módulo de saída digital fail-safe, no qual opera p. ex. um máquina com risco de perigo. Todas as outras saídas deste módulo de saída permanecem no seu status atual. Antes de ligar novamente a máquina, a chave de parada de emergência tem de ser reposta manualmente. Em seguida é necessário um sinal de confirmação. O fluxograma seguinte demonstra a relação.

Nota Neste exemplo, a máquina com risco de perigo é simulada por uma lâmpada de sinalização. Utilizando outros atuadores do que esta lâmpada de sinalização, o desligamento seguro dos consumidores inclusive a realimentação do sinal ainda tem de ser completado.

Para o cálculo do tempo de resposta máximo do seu sistema F utilize o aquivo Excel (tabela Cotia), que está à disposição para S7 Distributed Safety V 5.**3**. Pode encontrar este arquivo na internet:

http://www4.ad.siemens.de/ww/view/de

sob o número de identificação de artigo **19138505**

Para a realização da funcionalidade de parada de emergência foram utilizadas neste exemplo exclusivamente as operações lógicas de Distributed Safety. Alternativamente você pode acessar o bloco correspondente da biblioteca de Distributed Safety (a partir de Distributed Safety V5.3) para a realização.

2.1 Vantagens/benefícios para o cliente

- Esforços mínimos de fiação através da utilização de CPU S7 fail-safe e periferia descentralizada. Quanto mais funções de segurança são realizadas, mais importância ganha esta vantagem.
- É necessária somente uma CPU S7, porque as partes dos programas fail-safe e as partes standard decorrem coexistentemente na CPU.
- Programação do programa fail-safe com STEP 7 Engineering-Tools.
- Utilização da superfície de editor dentro do programa fail-safe, como se conhece do STEP 7.

3 Componentes necessárias

Componentes de hardware

Componente	Tipo	Dados de encomenda	Nº	Fabricante
Alimentação elétrica	PS307 5A	6ES73071EA00-0AA0	1	SIEMENS AG
CPU S7, utilizável para aplicações de segurança	CPU 315F-2DP	6ES7315-6FF01-0AB0	1	
Micro Memory Card	MMC 512 kB	6ES7953-8LJ10-0AA0	1	
Interface Module para ET 200M	IM 153-2	6ES7153-2AA02-0XB0	1	
Módulo de entrada digital	SM321 DI16xDC24V	6ES7321-7BH00-0AB0	1	
Módulo separador		6ES7195-7KF00-0XA0	1	
Módulo de entrada digital, fail-safe	SM326 DI24xDC24V	6ES7326-1BK00-0AB0	1	
Módulo de saída digital, fail-safe	SM326 DO10xDC24V/2A	6ES7326-2BF01-0AB0	1	
Rack	482,6 mm	6ES7390-1AE80-0AA0	2	
Opcional: Lâmpada de sinalização incl. lâmpada de incandescência	amarelo	3SB3217-6AA30	1	
Parada de emergência	Botão cogumelo 1NF	3SB3801-0DG3	1	
Contato (para parada de emergência)	1NF, conexão roscada	3SB3420-0C	1	
Botão de pressão	verde, 1NA	3SB3801-0DG3	2	

Nota

Com os componentes de hardware indicados foi testada a funcionalidade. Para tal podem também ser utilizados produtos semelhantes, distintos dos da lista acima (p. ex. um outro módulo de entrada digital). Neste caso, observe, por favor, que eventualmente será necessário efetuar alterações no código de exemplo (p. ex. outros endereços).

Software e tools de projeção

Componente	Tipo	Dados de encomenda	Nº	Fabricante
SIMATIC STEP 7	V5.3 + SP1	6ES7810-4CC07-0YA5	1	SIEMENS AG
SIMATIC Distributed Safety	V5.3	6ES7833-1FC01-0YA5	1	

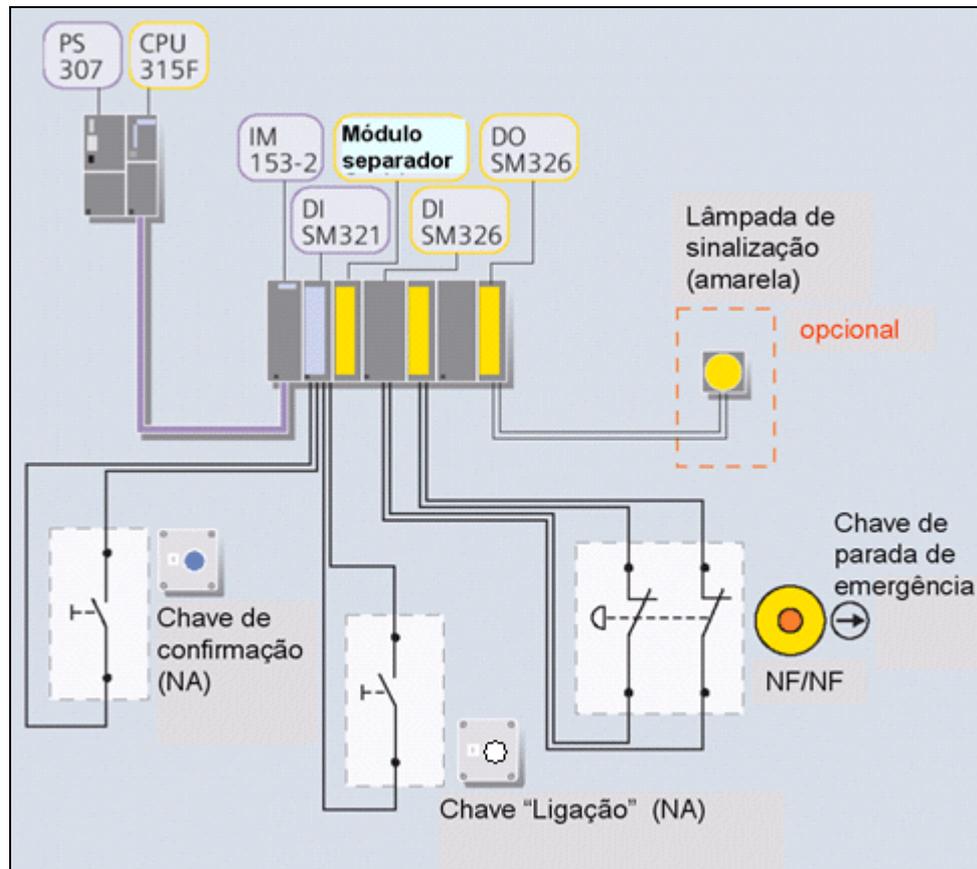
4 Montagem e fiação

É indispensável observar o seguinte aviso sobre a montagem e a fiação do exemplo de função:

Para atingir a categoria de segurança 4 é absolutamente indispensável realimentar o sinal de processo ao atuador. Neste exemplo, esta realimentação não é realizada.

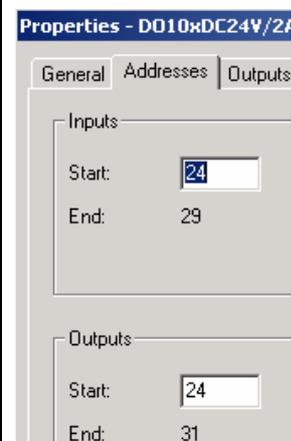
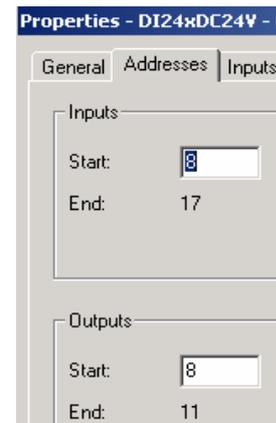
O atuador neste exemplo é uma lâmpada de sinalização que simula uma máquina. Na utilização de outros atuadores o próprio usuário terá de tratar da realimentação. O exemplo de função nº 7 trata explicitamente da temática "realimentação".

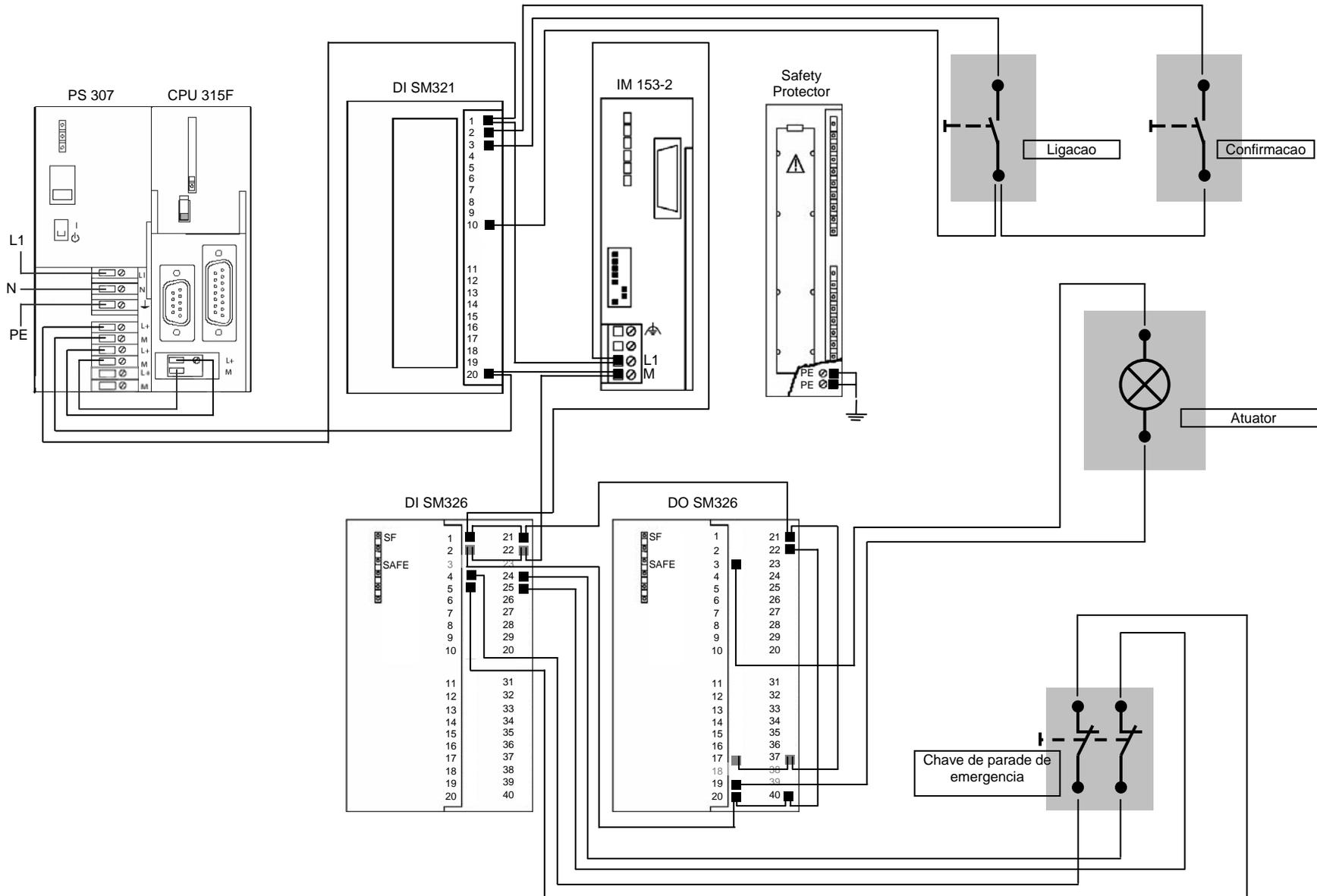
4.1 Esquema da montagem do hardware

O arranjo para realizar a funcionalidade da parada de emergência consiste numa configuração PROFIBUS. Nisto, uma CPU S7 fail-safe é utilizada como DP-Master, um ET 200M como DP-Slave. A lâmpada de sinalização utilizável opcionalmente simula uma máquina com risco de perigo. A lâmpada de sinalização pode ser substituída por um atuador conforme os seus requisitos.

4.2 Fiação do componentes de hardware

Condição: As alimentações elétricas são alimentadas com 230V AC.

Controle primeiramente os endereços ajustados nos componentes de hardware mencionados a seguir:

Componente de hardware	Endereço a ajustar	Nota	
IM 153-2	6 (endereço PROFIBUS)	Pode alterar	
DI (SM326)	8	É possível alterar as áreas de endereço do módulo através de introdução (chave DIL no verso do módulo). Porém, observe, por favor, o seguinte: No funcionamento de segurança o endereço de entrada e o endereço de saída têm de ser idênticos e divisíveis por oito e ter um valor entre 8 e 8176 (veja quadro)	Properties - DI24xDC24V - General Addresses Inputs Inputs Start: 8 End: 17 Outputs Start: 8 End: 11
DO (SM326)	24	É possível alterar as áreas de endereço do módulo através de introdução (chave DIL no verso do módulo). Porém, observe, por favor, o seguinte: No funcionamento de segurança o endereço de entrada e o endereço de saída têm de ser idênticos e divisíveis por oito e ter um valor entre 8 e 8176 (veja quadro)	Properties - DO10xDC24V/2A General Addresses Outputs Inputs Start: 24 End: 29 Outputs Start: 24 End: 31

Nota A interface DP da CPU 315F tem de ser ligada com a interface DP do IM 153-2.

PS 307
CPU 315F
DI SM321
IM 153-2
Safety
Protector
Ligacao
Confirmacao
L1
N
PE
Atuator
DI SM326
DO SM326
SF
SAFE
Chave de parade de
emergencia

Nota Para fazer o download do projeto S7 à CPU 315F-2DP necessita-se de uma ligação entre a interface MPI do Programador/PC e a interface MPI da CPU 315F-2DP (cabo MPI).

4.3 Teste de função

Depois da fiação dos componentes de hardware você pode (após carregar o projeto S7) testar as entradas e saídas utilizadas relativamente a sua funcionalidade.

Entradas e saídas utilizadas

Nº	Componente de hardware	Endereço	Símbolo	Sinal (valor default)	Nota
1	Chave (NA)	E 0.0	ACK	"0"	Confirmação
2	Chave (NA)	E 0.1	START	"0"	Ligação
3	Chave de parada de emergência (NF/NF)	E 8.0	ESTP	"1"	
4	Lâmpada de sinalização	A 24.0	ACTUATOR	"0"	"1": "Máquina" ativa

Testar as entradas e saídas

Condição: As entradas e saídas têm os valores default indicados sob "Entradas e saídas utilizadas".

Nº	Ação	Reação	Nota
		A 24.0	
1	Nenhuma	"0"	Depois da inicialização da CPU S7
2	Pressione ACK e solte a chave	"0"	Confirmação
3	Pressione START e solte a chave	"1"	"Máquina" (aqui simulada pela lâmpada de sinalização) em funcionamento
4	Pressione ESTP	"0"	Parada de emergência acionada

4.4 Ajustes importantes nos componentes de hardware

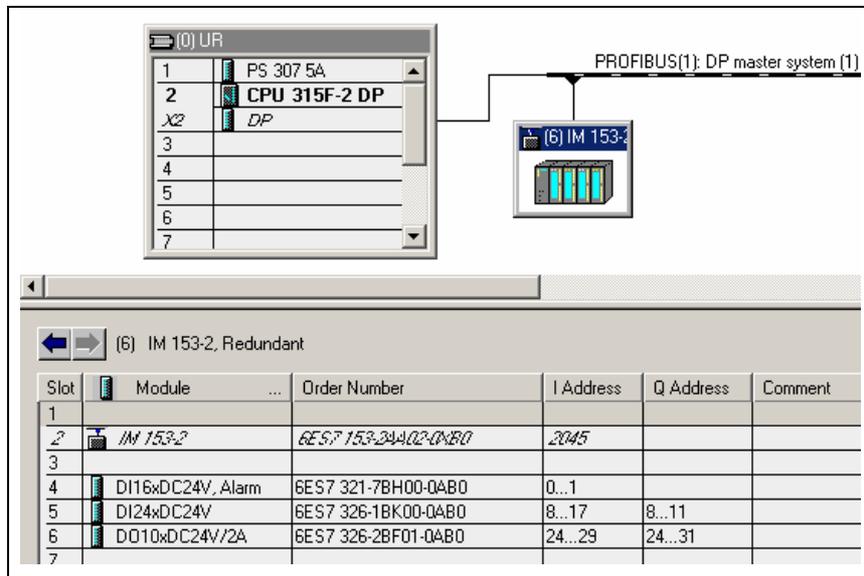
A seguir são apresentados alguns ajustes importantes da configuração de hardware de STEP 7 para dar uma vista geral. Estes ajustes encontram-se no projeto STEP 7 também fornecido. Por princípio, é possível efetuar alterações nestes ajustes (p. ex. devido a exigências individuais), mas, por favor, observe neste caso o seguinte aviso:

Atenção

Os ajustes indicados a seguir contribuem para o cumprimento da categoria de segurança 4. Alterações nos ajustes podem significar uma perda da função de segurança.

Se efetuar alterações (p. ex. acrescentar um outro módulo), tem de ser adaptado correspondentemente o código de exemplo.

O módulo separador não é indicado na configuração de hardware de STEP 7.

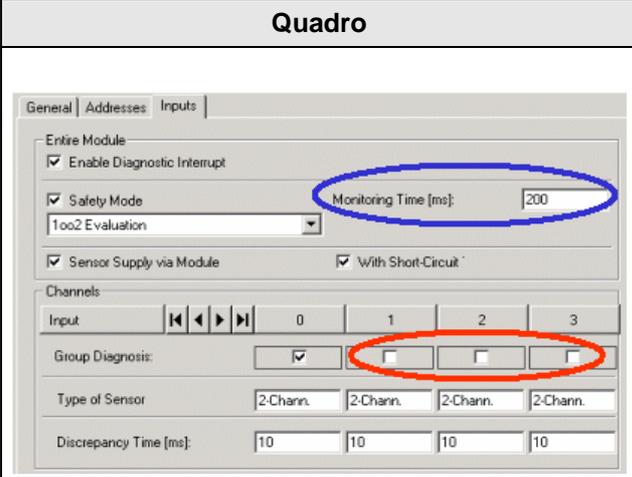
Quadro sinóptico

O endereço PROFIBUS é ajustado no IM 153 através de chave DIL.

Ajustes da CPU 315F-2DP

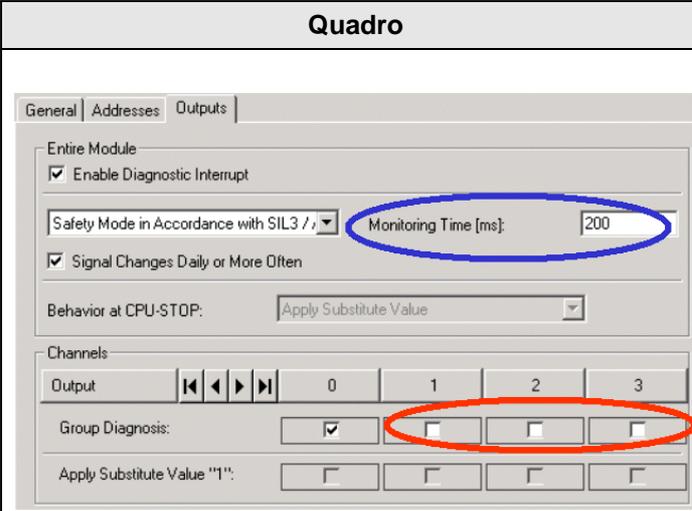
Acesso através de duplo clique em “CPU 315F-2 DP“ (veja “quadro sinóptico”).

Quadro	Nota
Cyclic Interrupt / Diagnostics/Clock Priority / Execution (ms) OB30: 7 / 5000 OB31: 8 / 2000 OB32: 9 / 1000 OB33: 10 / 500 OB34: 11 / 200 OB35: 12 / 50	Valor default 100 ms. Observe que o tempo de monitorização F tem de ser superior ao tempo de chamada do OB 35.
Level of Protection 1: Keyswitch Setting Removable with Password 2: Write-Protection 3: Write-/Read-Protection Password: ******** Enter Again: ******** CPU Contains Safety Program	Encontra-se no registro “Protection” É necessário atribuir uma senha para poder colocar o parâmetro “CPU Contains Safety Program“ (CPU contem programa de segurança). Apenas neste caso são gerados todos os blocos F necessários para o funcionamento seguro dos módulos F na compilação da configuração de hardware de STEP 7. A senha aqui utilizada: **siemens**

Ajustes do DI (SM 326) fail-safe

Acesso através de duplo clique em “DI24xDC24V” (veja “quadro sinóptico”).

Quadro	Nota
	Ajuste do “Monitoring time” (tempo de monitorização) Canais não utilizados tem de ser desativados.

Ajustes do DO (SM 326) fail-safe

Acesso através de duplo clique em “DO10xDC24V/2A” (veja “quadro sinóptico”).

Quadro	Nota
	Ajuste do “Monitoring time” (tempo de monitorização) Canais não utilizados tem de ser desativados.

5 Dados básicos de capacidade

Memória de carregamento e de trabalho (sem código de programa)

	Total	Blocos standard	Blocos F (fail-safe)
Memória de carregamento	cerca de 37,5	cerca de 0,2 k	cerca de 37,3 k
Memória de trabalho	cerca de 28,2	cerca de 0,08 k	cerca de 28,1 k

Memória de carregamento e de trabalho (com código de programa)

	Total	Blocos standard	Blocos F (fail-safe)
Memória de carregamento	cerca de 42,9 k	cerca de 1,1 k	cerca de 41,8 k
Memória de trabalho	cerca de 31,1 k	cerca de 0,4 k	cerca de 30,6 k

Tempo de ciclo

Tempo de ciclo total (típico)	cerca 5 ms	Programa standard e de segurança
Tempo de execução máximo do programa de segurança	10 ms	O cálculo é efetuado através da tabela Cotia. É indicado no capítulo 2 onde se encontra esta tabela.

6 Código de exemplo

Nota prévia

Junto oferecemos o projeto STEP 7 como código de exemplo, com o qual pode reproduzir a funcionalidade de parada de emergência aqui descrita.

O código de exemplo é sempre atribuído aos **componentes utilizados** no exemplo de função e realiza a funcionalidade exigida. Posições de problemas diferentes devem ser realizadas pelo usuário, podendo o código de exemplo servir de base.

Senha

As senhas utilizadas na parte relacionada à segurança são em todos os casos **siemens**.

Utilização do projeto STEP 7

Uma lâmpada de sinalização (simula uma máquina) é ligada através de uma chave (START). O desligamento efetua-se através de uma chave de parada de emergência. Para ligar novamente é necessário um sinal de confirmação (chave ACK).

Um desligamento condicionado pela operação não é realizado neste exemplo, sendo porém exposto nas páginas seguintes como é possível incluir este sinal.

Download

Para chamar o arquivo de projeto correspondente, abra o arquivo "as_fe_i_001_v10_code_estop.zip" oferecido como download separado (na página HTML) e extraia este para um diretório qualquer.

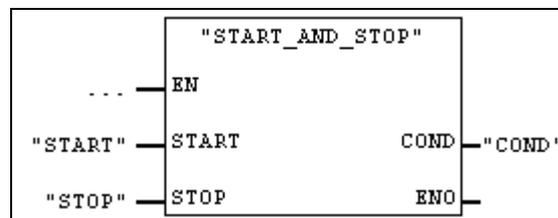
- Carregue primeiro a configuração de hardware na CPU S7.
- Mude para o SIMATIC Manager.
- Ative o diretório "Blocks" (Blocos)
- Menu "Options" (Opções) -> "Edit safety program" (Editar programa de segurança).
- Clique no botão "Download" (Fazer o download).
- Mude a chave dos modos de operação da CPU F de STOP para RUN.

O código de exemplo com as configurações indicadas possibilita o seguinte:

- Reinicialização de uma saída digital fail-safe depois de acionar a chave de parada de emergência.
- Para iniciar novamente (=início da aplicação) a saída digital fail-safe é necessário:
    1.) Confirmação pelo usuário (não implica automaticamente o início da aplicação).
    2.) Início da aplicação (somente possível com confirmação prévia)

Execução do programa

FC "START_AND_STOP" (FC10)

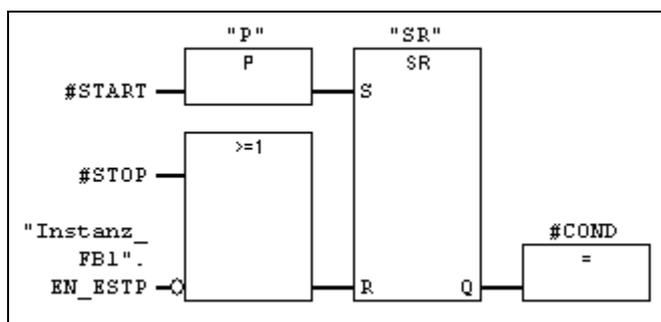
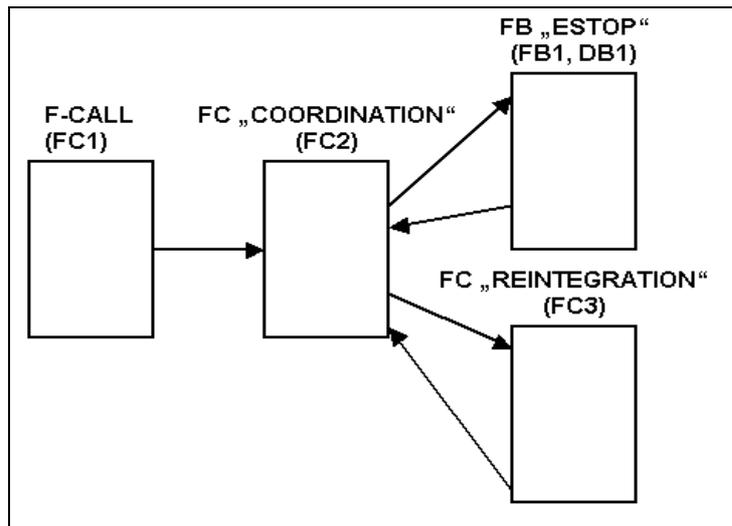
Do OB 1 é chamado o FC "START_AND_STOP" (FC 10) (não fail-safe)(veja quadro seguinte).

Parâmetro	Endereço	Descrição
START	E 0.1	Chave (NA) para requerer a ligação
STOP	M 90.5	Dummy. Se quiser realizar um desligamento condicionado pela operação, substitua o marcador por uma entrada Ex.y.
COND	M 90.0	Grava a informação ligação/desligamento da "máquina"

A informação do marcador “COND” é lido no programa de segurança como marcador COND 1. Esta atribuição efetua-se no alarme cíclico OB35 e tem a razão seguinte:

Se você quiser ler no programa de segurança dados do programa de usuário standard (marcador ou Imagem de Processo E da periferia standard) (aqui: COND) que durante a execução de um grupo de execução F podem ser alterados pelo programa de usuário standard ou um sistema de controle e monitorização, você tem de utilizar para isto marcadores próprios (aqui: COND1). Estes marcadores você tem de descrever imediatamente antes da chamada do grupo de execução F com os dados do programa de usuário standard. Neste caso pode acessar apenas estes marcadores no programa de segurança.

Neste exemplo isto já foi realizado. Geralmente, porém, tem validade:

Nota Se você não observar as frases acima, a CPU F pode mudar para STOP.

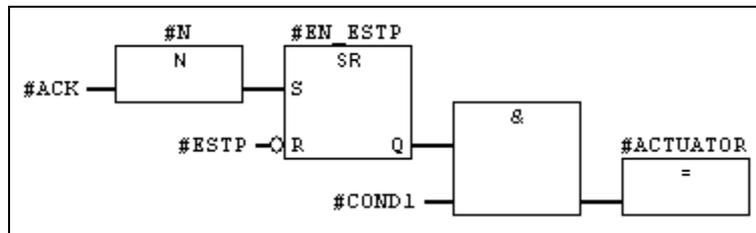
O FC “START_AND_STOP” (FC 10) no quadro seguinte inicia/reinicia #COND cujo status de sinal (“0” ou “1”) liga ou desliga a “máquina” no programa fail-safe. #COND somente pode tornar “1”, se a chave de parada de emergência for desbloqueada e confirmada antes da ligação (ocorre no programa de segurança). Isto é assegurado pelo bit “Instanz_FB1”.EN_ESTP do bloco de dados de instância DB 1 do FB 1 (do programa de segurança). Para uma ligação possível este bit tem de ser colocado. Se este bit for “0”, encontra-se o sinal “1” na entrada R do flip-flop, o que torna a saída Q sempre “0”, mesmo que com #START a entrada S recebe o sinal “1” (no flip-flop utilizado a reinicialização tem prioridade).

O programa fail-safe é executado como segue:

F-CALL (FC1)

O F-CALL (FC1) obrigatório é chamado do OB alarme cíclico (OB35) . Este chama o grupo de execução F (aqui o FC2).

FC “COORDINATION” (FC2)

Por razões da modularidade todos os outros blocos fail-safe são chamados a partir daqui.

FB “ESTOP” (FB1, DB1)

A parada de emergência é realizada como segue:

O status de sinal de #COND1 é definido no programa de usuário standard (veja FC 10 ou OB 35). #COND1=”1” é a primeira condição para a ligação da “máquina” (#ACTUATOR=”1”). A segunda condição é a confirmação necessária antes da ligação. Com #ACK=”1” é colocado o flip-flop (#EN_ESTP=”1”). A variável estática #EN_ESTP é lida no programa de usuário standard (FC 10) como bit do bloco de dados de instância do FB 1 e assegura assim que um sinal de ligação coloca ali apenas depois de uma confirmação o bit COND (ou COND1 no programa de segurança).

Pressionando a chave de parada de emergência torna #ESTP=“0” pelo que o flip-flop reinicia a saída Q em “0” (A reinicialização neste flip-flop tem prioridade), pelo que também #ACTUATOR torna “0”. (“Máquina” é desligada).

FC “REINTEGRATION” (FC3)

Este FC assegura a reintegração dos módulos fail-safe passivados (F-DI e/ou F-DO). Para o F-DO está preparado um bit marcador REINT que reintegra o módulo com um flanco positivo. A passivação é indicada por LED no módulo fail-safe. A reintegração de um módulo F pode demorar aproximadamente um minuto.

Advertência

Neste exemplo a reintegração de módulos passivados efetua-se automaticamente. Utilize a reintegração automática apenas se daí não resultar nenhum perigo.

Instruções de serviço

A tabela seguinte ajuda você na utilização.

Nº	Ação	Resultado / nota
1	Pressione a chave de confirmação ACK e solte-a	
2	Pressione a chave para a instrução de ligação START e solte-a	A lâmpada de sinalização acende (“máquina“ ativa)
3	Pressione a chave de parada de emergência	A lâmpada de sinalização apaga. A saída do módulo da saída digital fail-safe é **reiniciada**.
4	Desbloquear a chave de parada de emergência	Recomece com a ação 1.

Avaliação/feedback

A&D AS CS3 KM D-90327 Nürnberg-Moorenbrunn Fax: 0911 895 – 15 2407 E-mail: csweb@ad.siemens.com	
Remetente Nome: Repartição Local: Telefone: Endereço internet	Se você verificar erros ortográficos ao ler este documento, pedimos o favor de indicar-nos estes erros através deste formulário. Agradecemos também por contribuições de sugestões e propostas.

Avaliação do documento

Considero muito bom ❑ **Considero bom** ❑

Não considero bom ❑ **Porque**

..

Tema bem escolhido ❑ **Tema equivocado** ❑

Volume suficiente ❑ **Muito detalhado** ❑ **Muito superficial** ❑

Compreensível ❑ **Parcialmente compreensível** ❑ **Não compreensível** ❑

Boa realização ❑ **Média realização** ❑ **Má realização** ❑

Utilizado muitas vezes ❑ **Utilizado poucas vezes** ❑ **Apenas uma vez, depois já não** ❑

Economia de tempo pela utilização do documento em relação ao tempo anterior:

Nenhuma economia ❑ **cerca de 5%** ❑ **cerca de 10%** ❑ **outros...........%**

Sugestões: